EXHIBIT A

Michael R. Reese (State Bar No. 206773)
mreese@reesellp.com
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

George V. Granade (State Bar No. 316050)
ggranade@reesellp.com
REESE LLP
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Telephone: (310) 393-0070

Kevin Laukaitis (*pro hac vice* to be filed)
klaukaitis@laukaitislaw.com
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Telephone: (215) 789-4462

Counsel for Plaintiff
and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF ORANGE

Dhaman Gill, *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Case No. 30-2023-01357041-CU-BT-CXC

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Assigned for All Purposes
Judge Randall J. Sherman
Dept. CX105

Plaintiff Dhaman Gill ("Plaintiff") brings this class action complaint against Defendant 23andMe, Inc. ("Defendant"), for its failure to properly secure and safeguard the personally identifiable information ("PII") of Plaintiff and the members of the "Class" (defined below) that was stored within Defendant's information network.

INTRODUCTION

1. Defendant is a biotechnology company focusing on discovery of ancestral genetics.

2. Defendant acquired, collected, and stored Plaintiff's and the Class members' PII.

3. At all relevant times, Defendant knew, or should have known, that Plaintiff and the Class members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

4. On no later than October 6, 2023, unauthorized third-party cybercriminals gained access to the Class members' and, on information and belief, Plaintiff's PII as hosted with Defendant, with the intent of engaging in the misuse of the PII, including marketing, disseminating, and selling Plaintiff's and the Class members' PII (the "Data Breach").

5. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is unknown at this time but is estimated to be approximately 1,000,000 individuals at a minimum.

6. PII generally incorporates information that can be used to distinguish or trace an individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

7. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Defendant's information network, includes, without limitation: names, sex, birth year, genetic ancestry results, profile photos, and geographical location.

8. Defendant disregarded the rights of Plaintiff and the Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and the Class members' PII was safeguarded, failing

to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

9. As a result, the PII of Plaintiff (on information and belief) and the Class members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and the Class members in the future.

10. Plaintiff and the Class members have a continuing interest in ensuring that their information is and remains safe, and they therefore seek injunctive and other equitable relief.

JURISDICTION AND VENUE

1. **Personal Jurisdiction.** Defendant is both headquartered within the State of California and has purposefully availed itself of the privilege of doing business within the State. This action arises out of and relates to Defendant's contacts with this forum. Specifically, Defendant knowingly directed its services through the stream of commerce into this forum. Defendant has advertised and marketed within this forum through the wires and mails, and via mobile applications and websites through which residents of this forum can purchase Defendant's services and products. Defendant knowingly direct electronic activity into this forum with the intent to engage in business interactions and has in fact engaged in such interactions. Defendant offers services and products to consumers in this forum who made purchases using Defendant's services in this forum, and whose losses were incurred here. The Court has specific personal jurisdiction over Defendant as it can be said to have reasonably anticipated being hauled into court in this forum.

2. **Subject Matter Jurisdiction.** This Court has subject matter jurisdiction over this action pursuant to Article VI, section 10 of the California Constitution and Code of Civil Procedure section 410.10.

3. **Venue.** Venue is proper because Defendant conduct business in this county that brought about the business transactions at issue in this case. In addition, Plaintiff resides in this County. Additionally, a substantial part of the acts and conduct charged herein occurred in this

County. Venue also is proper because many Class members did business with Defendant and engaged in transaction in this County, and Defendant has reaped substantial profits from customers who engaged in transactions in this County.

THE PARTIES

Plaintiff Dhaman Gill

11. Plaintiff Dhaman Gill is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in Newport Beach, Florida. On information and belief, Plaintiff is a victim of the Data Breach.

12. Plaintiff initially signed up for Defendant's services in or about December 2018 and has paid approximately $50.00 as a customer of Defendant's, and his information was stored with Defendant as a result of his dealings with Defendant.

13. As required in order to obtain services from Defendant, Plaintiff provided Defendant with highly sensitive personal information, including a DNA sample, and Defendant then possessed and controlled that sensitive personal information.

14. As a result, on information and belief, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

15. At all times herein relevant, Plaintiff is and was a member of the Class.

16. Plaintiff received an email from Defendant, dated October 10, 2023, notifying Plaintiff of the Data Breach and that the Plaintiff's information was among that compromised (together, the "Notice").

17. The Notice attempts to redirect the blame on to the criminal actors that gained access to Defendant's customer accounts.

18. The first email in the Notice avoided mentioning that Defendant's safeguards were inadequate.

19. Though the second email discussed the safeguards, it did not note the inadequacies that allowed the Data Breach to occur.

20. The Notice is deficient for several reasons: (i) Defendant fails to state definitively if it was able to contain or end the cybersecurity threat, leaving victims to fear whether the PII that

Defendant continues to maintain is secure; and (ii) Defendant fails to state definitively how the breach itself occurred. This information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

21. As a result of the Data Breach, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny and time spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach.

22. Plaintiff was also injured by the material risk to future harm he suffers based on Defendant's Data Breach; this risk is imminent and substantial because (i) on information and belief, Plaintiff's data has been exposed in the Data Breach; (ii) the data involved is highly sensitive and presents a high risk of identity theft or fraud; and (iii) it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused, including Plaintiff's PII.

23. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a condition of intangible property that he entrusted to Defendant, which, on information and belief, was compromised in and as a result of the Data Breach.

24. Plaintiff, as a result of the Data Breach, has increased anxiety for his loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII.

25. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from, on information and belief, his PII being placed in the hands of unauthorized third parties/criminals.

26. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant 23andMe, Inc.

27. Defendant 23andMe, Inc., has its principal place of business located at 223 North Mathilda Avenue, Sunnyvale, California 94086.

CLASS ACTION ALLEGATIONS

28. Pursuant to California Code of Civil Procedure section 382, Plaintiff brings this action on behalf of the proposed Classes defined as follows:

The California Class. All California residents whose PII was exposed to unauthorized third parties as a result of the Data Breach experienced by Defendant.

29. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

30. Plaintiff reserves the right to amend the above definition in subsequent pleadings and motions for class certification.

31. Certification of Plaintiff's claims for class-wide treatment is appropriate because the questions presented are of a common and general interest, and the parties are so numerous that it is impracticable to bring them all before the court and because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as individual Class members would use to prove those elements in individual actions alleging the same claims.

32. The size of the Classes is so large that joinder of all Class members is impracticable. Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the classes will be determined by analysis of Defendants' records.

33. Questions of law and fact of common and general interest to the Class predominate over any questions that affect only individual Class members. Common legal and factual questions/issues include but are not limited to:

a. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of the PII of Plaintiff and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

34. Defendant engaged in a common course of conduct in contravention of the laws Plaintiff seeks to enforce individually and on behalf of the Class. Similar or identical

violations of law, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the predominant common questions. Moreover, the common questions will yield common answers that will substantially advance the resolution of the case.

35. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

36. There are no defenses available to Defendant that are unique to the named Plaintiff.

37. Plaintiff is a fair and adequate representative of the Class because Plaintiff's interests do not conflict with the Class members' interests. Plaintiff will prosecute this action vigorously and is highly motivated to seek redress against Defendant. Furthermore, Plaintiff has selected competent counsel who are experienced in class actions and other complex litigation, including data breach class actions. Plaintiff and Plaintiff's counsel are committed to prosecuting this action vigorously on behalf of the Class and have the resources to do so.

38. The class action mechanism is superior to other available means for the fair and efficient adjudication of this controversy for reasons including but not limited to the following:

    a. The damages individual Class members suffered are small compared to the burden and expense of individual prosecution of the complex and extensive litigation needed to address Defendant's misconduct.

    b. It would be virtually impossible for the Class members individually to redress effectively the wrongs done to them. Even if Class members themselves could afford such individual litigation, the court system could not. Individualized litigation would unnecessarily increase the delay and expense to all parties and to the court system and presents a potential for inconsistent or contradictory rulings and judgments. By contrast, the class action device presents far fewer management difficulties, allows the hearing of claims which might otherwise

go unaddressed because of the relative expense of bringing individual lawsuits, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

c. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for Defendant.

d. The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications or that would substantively impair or impede their ability to protect their interests.

39. Defendant has acted on grounds applicable to the Class as a whole, so that final injunctive and declaratory relief concerning the Class as a whole are appropriate.

40. Plaintiff suffers threat of future harm because unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII and/or financial information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

41. Plaintiff and Plaintiff's counsel anticipate that notice to the proposed Class will be effectuated through recognized, Court-approved notice dissemination methods, which may include United States mail, electronic mail, Internet postings, Social media, and/or published notice.

NO DIVERSITY OR FEDERAL JURISDICTION

There is no diversity between Defendant, Plaintiff or other members of the Class and nothing in this Complaint should be interpreted to convey diversity. Accordingly, there is no federal jurisdiction that this state should be litigated in California state court.

COMMON FACTUAL ALLEGATIONS

Defendant Failed to Protect Plaintiff's and the Class Members' PII

42. Unauthorized third-party cybercriminals gained access to the Class members' and, upon information and belief, Plaintiff's PII with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and the Class members' PII.

43. Defendant had and continues to have obligations created by applicable state law, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and the Class members' PII confidential and to protect such PII from unauthorized access.

44. Plaintiff and the Class members were required to provide their PII to Defendant as a part of using its services, and in so requiring, Defendant created the reasonable expectation and mutual understanding with Plaintiff and the Class members that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

45. Plaintiff and the Class members remain in the dark regarding the full exact details of, among other things, what particular data was stolen, how, and by whom.

46. Plaintiff and the Class members are, thus, left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

47. Unauthorized individuals can now easily access the PII of the Class members and, upon information and belief, Plaintiff.

Defendant Collected/Stored Class Members' PII

48. Defendant acquired, collected, and stored and assured reasonable security over Plaintiff's and the Class members' PII.

49. As a condition of its relationships with Plaintiff and the Class members, Defendant required that Plaintiff and the Class members entrust Defendant with highly sensitive and confidential PII.

50. Defendant, in turn, stored that information in the part of Defendant's system that

was ultimately affected by the Data Breach.

51. By obtaining, collecting, and storing Plaintiff's and the Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was thereafter responsible for protecting Plaintiff's and the Class members' PII from unauthorized disclosure.

52. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII.

53. Plaintiff and the Class members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

54. On information and belief, Defendant could have prevented the Data Breach, which began no later than October 6, 2023, by adequately monitoring, securing, encrypting, and/or more securely encrypting its servers generally, as well as Plaintiff's and the Class members' PII, and/or could have required two-factor authentication.

55. Defendant's negligence in safeguarding Plaintiff's and the Class members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

56. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take sufficient steps to protect Plaintiff's and the Class members' PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

57. Defendant's failure to adequately secure Plaintiff's and the Class members' sensitive data breaches duties it owes Plaintiff and the Class members under statutory and common law. Moreover, Plaintiff and the Class members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

58. Defendant owed a duty to Plaintiff and the Class members to exercise reasonable

care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

59. Defendant owed a duty to Plaintiff and the Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and the Class members.

60. Defendant owed a duty to Plaintiff and the Class members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII was adequately secured and protected.

61. Defendant owed a duty to Plaintiff and the Class members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

62. Defendant owed a duty to Plaintiff and the Class members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

63. Defendant owed a duty to Plaintiff and the Class members to act upon data security warnings and alerts in a timely fashion.

64. Defendant owed a duty to Plaintiff and the Class members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

65. Defendant owed a duty of care to Plaintiff and the Class members because they were foreseeable and probable victims of any inadequate data security practices.

66. Defendant owed a duty to Plaintiff and the Class members to encrypt and/or more reliably encrypt Plaintiff's and the Class members' PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

67. PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal

information on several underground internet websites.

68. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[1]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[2]; and other sources report that criminals can also purchase access to entire company data breaches for $900 to $4,500.[3]

69. Identity thieves can use PII, such as that of Plaintiff and the Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

70. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[4]

71. Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and the Class members' PII were stolen, including the significant costs that would be placed on Plaintiff and the Class members as a result of a breach of this magnitude.

---

[1] Anita George, DIGITAL TRENDS, *Your personal data is for sale on the dark web. Here's how much it costs* (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ [https://perma.cc/254V-5VNE].

[2] Brian Stack, EXPERIAN, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [https://perma.cc/8XCU-E8ET].

[3] *In the Dark*, VPNOVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ [https://perma.cc/D8KZ-HPBW].

[4] GAO, *Report to Congressional Requesters*, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf [https://perma.cc/5636-3YPB].

72. Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and the Class members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

73. Defendant disregarded the rights of Plaintiff and the Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and the Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and/or extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and the Class members prompt and accurate notice of the Data Breach.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
On Behalf of the Class

74. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

75. At all times herein relevant, Defendant owed Plaintiff and the Class members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiff and the Class members in its computer systems and on its networks.

76. Among these duties, Defendant was expected:

i. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession;

ii. to protect Plaintiff's and the Class members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

iii. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

iv. to promptly notify Plaintiff and the Class members of any data breach,

security incident, or intrusion that affected or may have affected their PII.

77. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and the Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

78. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

79. Defendant knew, or should have known, about numerous, well-publicized data breaches.

80. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and the Class members' PII.

81. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and the Class members had entrusted to it.

82. Defendant breached its duties to Plaintiff and the Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

83. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and the Class members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

84. Plaintiff's and the Class members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions.

85. Moreover, only Defendant had the ability to protect its systems and the PII is stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and the Class members.

86. Defendant also had independent duties under state laws that required Defendant to reasonably safeguard Plaintiff's and the Class members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

87. Defendant breached its general duty of care to Plaintiff and the Class members in, but not necessarily limited to, the following ways:

i. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and the Class members;

ii. by failing to timely and accurately disclose that Plaintiff's and the Class members' PII had been improperly acquired or accessed;

iii. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

iv. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and the Class members, misuse the PII and intentionally disclose it to others without consent;

v. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class members' PII;

vi. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

vii. by failing to encrypt Plaintiff's and the Class members' PII and monitor user behavior and activity in order to identify possible threats.

88. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

89. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class members have suffered damages and are at imminent risk of additional harms and damages.

90. To date, Defendant has not provided sufficient information to Plaintiff and the Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class members.

91. Further, through its failure to provide clear notification of the Data Breach to Plaintiff and the Class members, Defendant prevented Plaintiff and the Class members from taking meaningful, proactive steps to secure their PII.

92. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class members and the harm suffered, or

risk of imminent harm suffered, by Plaintiff and the Class members.

93. Plaintiff's and the Class members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

94. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

95. The damages Plaintiff and the Class members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

96. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and the Class members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class members.

97. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

98. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class members have suffered and will suffer the continued risks of exposure of their PII,

which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT TWO
Unjust Enrichment
On Behalf of the Class

99. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

100. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and the Class members.

101. Defendant, prior to and at the time Plaintiff and the Class members entrusted their PII to Defendant for the purpose of obtaining Defendant's services, caused Plaintiff and the Class members to reasonably believe that Defendant would keep such PII secure.

102. Defendant was aware, or should have been aware, that reasonable consumers would have wanted their PII kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were substandard for that purpose.

103. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and the Class members' decisions to seek services from Defendant.

104. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and the Class members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

105. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and the Class members the ability to make a rational and informed purchasing decision and took undue advantage of Plaintiff and the Class members.

106. Defendant was unjustly enriched at the expense of Plaintiff and the Class members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and

the Class members; however, Plaintiff and the Class members did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

107. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation, or profits it realized from these transactions.

108. Plaintiff and the Class members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and the Class members may seek restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of each member of the proposed Class, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and for the following specific relief against Defendant:

A. that the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed Class including the appointment of Plaintiff as Class representative and Plaintiff's counsel as Class counsel;

B. for an award of restitution and damages (though Plaintiff specifically does not seek damages under the CLRA or CCPA, though reserves the right to amend to seek damages under those statutes once notice is provided to Defendant and if Defendant fails to comply with the requirements of the CLRA and CCPA notice), as allowed by law in an amount to be determined;

C. that the Court enjoin Defendant, ordering it to cease from unlawful activities;

D. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class members;

E. for injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class members,

including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business;

iii. requiring Defendant to delete and purge the PII of Plaintiff and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and the Class members' PII;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

vi. prohibiting Defendant from maintaining Plaintiff's and the Class members' PII on a cloud-based database;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and the Class members;

x. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xi. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

xii. requiring Defendant to meaningfully educate all Class members about the threats they face due to the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

F. for pre- and post-judgment interest on all amounts awarded, at the prevailing legal rate;

G. for an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

H. for all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Date: October 25, 2023

Respectfully submitted,

REESE LLP

By: */s/ Michael R. Reese*
Michael R. Reese (State Bar No. 206773)
mreese@reesellp.com
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

REESE LLP
George V. Granade (State Bar No. 316050)
ggranade@reesellp.com
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Telephone: (310) 393-0070

Kevin Laukaitis (*pro hac vice* to be filed)
klaukaitis@laukaitislaw.com
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Telephone: (215) 789-4462

Counsel for Plaintiff and the Proposed Class